Enough Already!

Protect Yourself from Online
Political Manipulation and
False News in Election 2018

BY JEFF CHESTER, STEVEN ROSENFELD AND
THE CENTER FOR DIGITAL DEMOCRACY

Table of Contents

Note to Readers

This brief guide aims to help you understand what happened in 2016, explaining how online media — especially advertising on top social media platforms — drove some of the worst features of the nastiest presidential campaign this century. This guide seeks to explain the way online media enticed and magnified this noise, and what people can do now to try to insulate themselves from these forces in 2018's midterm election and a rapidly approaching 2020 presidential race.

How Elections Have Changed: What 2016 Taught Us

What Trump Was Able to Accomplish with Social Media

*A*s the 2016 presidential election crested, two Bloomberg reporters, Joshua Green and Sasha Issenberg, gave the world its *first detailed look* at the digital voter-targeting operation inside Donald Trump's campaign.[1]

Until then, many political reporters assumed it was Hillary Clinton's campaign that was being directed by online whizzes, while Trump was "running one of the most analog campaigns in recent history," as the *Washington Post* had put it in late August.[2] That storyline was flat-out wrong. One of Trump's best-kept secrets was an unprecedented online effort to identify and target persuadable voters.[3] For months they had been bombarded with finely tuned content, mostly via social media, to engage and provoke their personal biases, regardless of its factual accuracy.

"Twitter is how [Trump] talked to the people; Facebook was going to be how he won," recounted Trump's digital director, Brad Parscale, on CBS's *60 Minutes*, a year after the election.[4] (In 2018, Trump named Parscale as his 2020 presidential campaign manager.)

Trump's use of advances in digital data mining, online advertising and social media platforms was not unique in 2016. The way that his team used this digital technology was part of a larger trend of more direct, manipulative

and extremist campaigning—including the outbreak of online propaganda. These trends are continuing as 2018's midterms approach and will likely follow into 2020's presidential contest.

Trump's campaign had accepted offers from Facebook, Twitter and Google to have employees—technical and advertising experts—work in his digital operation center.[5] Katie Harbath, Facebook's global politics and government outreach director, told academic researchers after the election that her colleagues were sympathetic to their candidate, and their role was showing the Trump team "how to use the product the best way."[6] Hillary Clinton's campaign declined the offer, possibly because she had social media veterans among her staff.[7]

CLINTON SPENT $28 MILLION, TESTING 66,000 ADS. TRUMP SPENT $44 MILLION, TESTING 5.9 MILLION ADS.

The embedded Silicon Valley employees helped Trump's team find and contact swing voters in must-win states. According to Parscale, Facebook was pivotal. The social media platform, with more than 210 million American users[8] and an elaborate advertising system based on profiling and deeply tracking users, also lets advertisers put their data into its audience targeting system. Trump's team inputted Republican National Committee voter files and other data.[9] Their goal was to find voters—sometimes as few as 15 at a time—in key locales. When these Facebook users visited the platform,
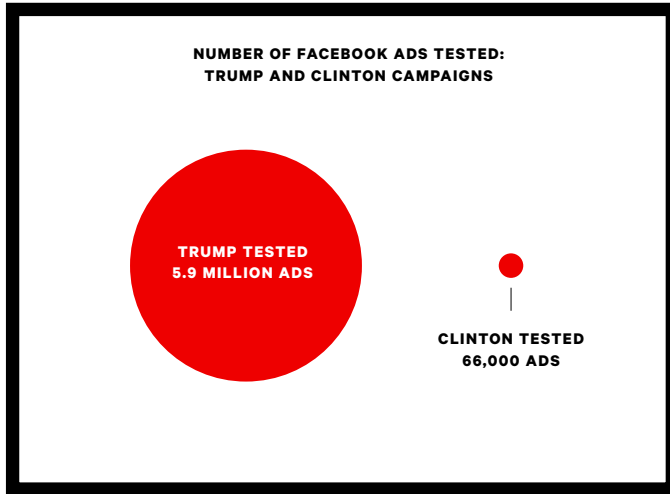
they would see paid posts attuned to their presumed politics and personalities.

Trump's campaign used Facebook's data-driven system—built on a basic Silicon Valley business model—to send out thousands of micro-targeted political messages daily. The system tracked which posts prompted responses and which did not, so they could keep refining prods, pitches and provocations. Parscale saw Facebook's data, advertising and platform as the epicenter of a vast political targeting, engagement and propaganda apparatus. Clinton's campaign, in contrast, viewed Facebook simply as one of many tools to use.

Statistics point to these different strategies. From June to November 2016, the Clinton campaign spent $28 million on Facebook, testing variables on 66,000 ads. In contrast, Trump's campaign spent $44 million and tested 5.9 million ads.[10] As Epolitics observed, Parscale "was effectively in charge of the campaign's entire outreach/advertising program by the end."[11]

The 2016 presidential election was a turning point in American politics for many reasons. Chief among them was a growing realization that the giant digital platforms that help millions of people socialize and communicate had become a primary means for spreading partisan vitriol, worsening already polarized politics and increasing the power of disruptive extremists.

Stanford Law School's Nathaniel Persily, a nationally known election law scholar, addressed the emerging danger in the *Journal of Democracy* in spring 2017. "From the point of view of the health of liberal democracy, the

**NUMBER OF FACEBOOK ADS TESTED:
TRUMP AND CLINTON CAMPAIGNS**

TRUMP TESTED
5.9 MILLION ADS

CLINTON TESTED
66,000 ADS

Internet's great promises are also its pitfalls," Persily writes. "Its liberating, anti-establishment potential can be harnessed by demagogues who appeal to the worst impulses of the mob."[12]

Online media platforms have a positive side and dark side. On one hand, their emergence has been revolutionary for political organizing, sociologist and computer scientist Zynep Tufecki wrote in her 2017 book, *Twitter and Tear Gas: The Power and Fragility of Networked Protest*.[13] They can function as coffee shop, alternative press, bulletin board and political wire — when used benevolently. But major platforms like Facebook, Twitter and YouTube have a dark side, she also noted, because they have unleashed a flood of "misinformation, information glut, doubt, confusion, harassment, and distraction, making it hard for ordinary people to navigate the networked public sphere, and sort facts from fiction, truth from hoaxes."

In recent national elections, online communication has become increasingly important to campaigns. No serious candidate can now be without an online organizing and social media presence. But in 2016, digital data, advertising and platforms "combined to upset established paradigms of how to run for president," as Persily noted.[14]

This guide seeks to explain what happened and what voters can do about it—as people now spend an average of 5.9 hours a day online, with 3.3 of those hours on their mobile devices.[15]

Throughout the 2016 campaign, there was mounting evidence that online organizing and advertising would play an outsized role. This could be seen in the most traditional political success metric—fundraising. Digital posts, including paid ads, prompt people to reply by email, which is the key to raising money.[16] Early on and throughout the campaign, Trump was more successful with online fundraising than his rivals. By Election Day, his campaign had raised $240 million in small donations (under $200), compared to Clinton's $137 million.[17]

Digital Voter Suppression

P arscale's team also used social media advertising tools for a dirty tactic—"three major voter suppression operations," as an unnamed "senior official" told Bloomberg two weeks before Election Day.[18] Combining data from the RNC, GOP lists and Facebook's advertising system, the Trump campaign identified swing-state voters to be hit with political mud. As Bloomberg noted, they targeted "idealistic white liberals [likely Bernie Sanders supporters], young women [likely offended by Trump's misogyny] and Blacks [assumed Democrats]" for paid posts to discourage voting.[19]

They also used Facebook to send "dark" ads—only visible to recipients. The Berniecrats were urged to vote for Jill Stein, the Green candidate. Blacks were reminded Clinton had once called gang members "super-predators." Florida's Haitians were reminded about botched Clinton Foundation projects. The Black Lives Matter movement was attacked.[20] Other minorities, such as Muslim-Americans, were also smeared in incendiary missives.

"THE INTERNET'S GREAT PROMISES ARE ALSO ITS PITFALLS. ITS LIBERATING, ANTI-ESTABLISHMENT POTENTIAL CAN BE HARNESSED BY DEMAGOGUES WHO APPEAL TO THE WORST IMPULSES OF THE MOB."

Negative campaigning and late-breaking attacks are not new. What was new in 2016 was the way online media's targeting and reach were used in America (and overseas) to provoke and exploit polarization—including directly by the Trump campaign.

But Trump wasn't alone. His effort was the tip of a larger digital spear wielded by extreme partisans, domestic provocateurs and even Russian agents. People post all kinds of material online that goes unnoticed, but these online campaigns had a profound impact. They inflamed passions. They prompted reactions. Missives based on deliberately false information were lapped up, shared and circulated, many metrics measuring these activities showed. Silicon Valley's business model, crafted to know people's inclinations and grab their attention, was working.

Consider three examples:

- *Trump and his aides routinely tweeted his most inflammatory taunts from rallies, which were retweeted at three times the rate of Clinton's messages.[21] This statistic shows the nature of what makes content go viral; how a provocative tweet spreads more quickly, especially if senders are passionate.*

- *Drawn by the ease of accessing and profiting from automated online advertising systems, teenagers in Eastern Europe created and posted increasingly outrageous pro-Trump and anti-Clinton stories, such as claims that an FBI agent was killed after leaking Clinton's emails, on about 140 websites, earning $30,000 a month.[22] This shows the failure of Facebook and others to create safeguards for their automated ad apparatus, allowing it to be easily gamed, so as not to diminish any revenues.*

> • *Mike Cernovich, a domestic right-wing provocateur, used the platforms to spread brazen lies—such as the "Pizzagate" conspiracy, where he claimed liberal politicians were molesting children in a District of Columbia pizzeria. That prompted a North Carolina man to travel to Washington and fire a rifle at the restaurant.[23] This shows how political trolling was empowered.*

These incidents were part of a larger trend that was fueled by, and blossomed, on the platforms: the epidemic of what is called "fake news"—although many people prefer to call it junk news, false news, disinformation, or propaganda, to avoid sounding like Donald Trump, who co-opted the phrase during the campaign.

In 2016, Americans were engaging in politics through an online window as never before. But much of what they saw, shared and spread on social media was warped. A week after the election, *BuzzfeedNews* reported the "top fake election news stories generated more total engagement on Facebook than top election stories from 19 major news outlets combined."[24]

Russian intelligence operatives also saw how the Internet and online media's architecture could roil their rivals' domestic politics. The 2016 version of the 1972 Watergate break-in by President Richard Nixon's henchmen (including intelligence agents) to steal Democratic National Committee campaign plans was the hacking and theft of emails inside the DNC and Clinton campaign. (These activities are detailed in Special Counsel Robert Mueller's indictment of 12 Russians in July 2018.)[25] However, Nixon's burglars and intelligence operatives did not have online advertising tools.

New Paths to Propaganda and Extreme Politics

F acebook's advertising options allowed Trump's team to home in on key locations and create "lookalike" targets of apparently like-minded people to be sent a range of ads. This system allows anyone buying an ad to find recipients by "cloning" sought-after traits. Recipients never know they have been tagged by a black-box system—the hidden coding of their personality and psychology as gleaned from their online activities.

Trump's team also understood another key social media feature attuned to a deep part of human nature: the realization that people were prone to believe almost anything if it was seen as coming from someone like them.[26] This is the basis for how propaganda spreads among an uncritical public.

"They understood [the appearance of] authenticity over truth," as technology writer Melissa Ryan noted after the election.[27] "They were banking that people are more likely to believe something from an unofficial source that seems true than something from an official source that actually is true."

This is an important point. Many editorials criticized Trump for a lack of policy detail and inattention to facts. Those critics did not realize that the candidate and campaign chose to emphasize a different kind of content at rallies and online: anything that grabbed the audience's attention and got a reaction. Targeted engagement, regardless of facts, is what online advertising was

designed to promote. In business, that dynamic leads to sales. In politics, it promotes many things, including vitriol and polarization if used manipulatively.

Ryan further observed that the social media posts by Trump supporters and right-wing websites offered a trove of incendiary content to be recycled by the campaign, which it did. "They were also masters at spreading false news stories, rumors, and conspiracy theories packaged for a mass audience via social media," she wrote.[28]

In his 2017 *Journal of Democracy* article, Stanford's Persily cited research showing Trump's campaign sought to create an online echo chamber, what technologists call a "filter bubble." Persily noted that 20 percent of Trump's tweets were "retweets of the general public['s tweets], and roughly half his tweets contained links to other news media, as did 78 percent of his Facebook Posts."[29] In other words, Trump was circulating a lot of content that mirrored what recipients had said, or that sounded like them.

"THEY WERE BANKING THAT PEOPLE ARE MORE LIKELY TO BELIEVE SOMETHING FROM AN UNOFFICIAL SOURCE THAT SEEMS TRUE THAN SOMETHING FROM AN OFFICIAL SOURCE THAT ACTUALLY IS TRUE."

What emerged in 2016 was not a "Frankenstein moment" for Silicon Valley, where an innocent "creature has gone rogue," as a *New York Times* analyst wrote.[30] On the contrary,

this demon was always lurking in the platform's design and business model. For online platforms to be free to their users, and generate skyrocketing revenues, advertising's consumer data business model was embraced.

Whether it was Russia, Trump's campaign on a larger scale, or other 2016 campaigns, including Democratic office-seekers, the savviest operatives used every option that surveillance- and advertising-based business model offered. The official industry terms are programmatic advertising, geo-location, app tracking, mobile marketing, and more. (These are described in greater detail in Section 2.) What recipients saw were political messages that seeped into the familiar content they visited: pages, posts, images, videos, memes, tweets, texts, etc.

This manipulative template has only deepened since 2016, as political consultants keep looking for ever-more-immediate means to grab people's attention. In 2017, for the first time, spending on global digital advertising exceeded spending on traditional television.[31] As time passes, the use and variety of online tools, including negative campaigning, has grown. The British-based Oxford Internet Institute found evidence in 48 countries in 2018 of "formally organized social media manipulation," up from 28 countries in 2017.[32]

Needless to say, there has been a growing awareness of these trends and resultant efforts to rein them in. In Europe, where democratic governments have been paying more attention than Washington, there is a determination to track and address online incitements. The role of data surveillance in elections—especially content fanning conflict or misleading voters—is also being seriously

addressed. Unlike Americans, Europeans have memories of what life was like under fascism and communism. They recognize that the skin holding societies together can be torn apart. (A recent German study of 3,335 attacks on refugees in the past two years found towns with higher Facebook usage had the most racial violence.)[33]

The tendency to ignore the problem may be starting to shift in Congress.[34] In England, the government appears to be confronting it head on.

A British Parliament report in mid-2018 referred to online media's power to sow conflict.[35] "Arguably, more invasive than obviously false information is the relentless targeting of hyper-partisan views, which play to the fears and prejudices of people in order to influence their voting plans and their behavior. We are faced with a crisis concerning the use of data, the manipulation of our data, and the targeting of pernicious views."

Sarah Golding, the president of the Institute of Practitioners in Advertising, a British organization that recently called for a moratorium on political micro-targeting, told *The New York Times*[36] that Facebook "has essentially weaponized ad technology designed for consumer products and services.

"There is a danger that every single person can get their own concerns played back to them," she said.

In 2018, the most-visited platforms are taking some steps to police the most incendiary content their users post. Some are beginning to require political advertisers to reveal who is paying for the ads and who is being

targeted. As of mid-August, Facebook removed nearly 700 "fake accounts, pages and groups," some tied to foreign governments targeting audiences in the U.S. and abroad, for sowing misinformation.[37]

[FACEBOOK] HAS ESSENTIALLY WEAPONIZED AD TECHNOLOGY DESIGNED FOR CONSUMER PRODUCTS AND SERVICES"

But political operatives already are skirting these steps,[38] which is what aggressive campaigners have always done. In mid-2018, campaigns around the world have turned to using texts globally[39] and in the U.S.[40] to reach voters. What messaging pathways will be used in the 2020 presidential race is anybody's guess—but Parscale has pointed to more video.[41] That would be mean more personalized and targeted videos from YouTube, Facebook Live, and streams from cable and Internet providers.

The Challenges Elections and Democracy Face Today

Introduction

*A*s the 2018 mid-term elections approach, voters will need a higher level of awareness in order to navigate the turbulent political and social media reality, in the face of alarming amounts of false news, disinformation and advanced micro-targeting borrowed from the commercial sphere. We can expect even more sophisticated techniques and chicanery in 2020's presidential election, revisiting and updating some of 2016's most loathsome moments.

Our goal is to help you, the reader, be better prepared for these elections in light of the new realities of media manipulation. But it is important to step back for a moment and understand how the problems with modern political campaigns stem from much larger issues of the "surveillance economy," where data is collected non-stop whenever we use the Internet — or even just carry a smart phone in our pocket.

The Surveillance Economy

The world of technology has changed dramatically and the public and politicians are playing catch up. "Big data," including computer files that document the details of our lives, is now a dominant force of global capitalism.[2] According to the U.K. *Guardian*, "The flow of data now contributes more to world GDP [gross domestic product] than the flow of physical goods... This is a big shift – and one that has yet to fully sink in

for most people. Corporate America, on the other hand, understands it well."[43]

From the critics' point of view, the giants of digital technology have succeeded at unimagined levels. As the *Center for Digital Democracy* has extensively noted,[44] the results include monopolistic dominance, massive collection and abuse of personal data, device addiction, explosions in propaganda marked by a new prevalence and wide distribution of fake news, racist and right-wing memes, and a marginalization of progressive media and voices.

The Loss of Privacy

To understand the dark side of the data revolution, we have much to consider. Today, people are socialized to share the details of their lives on social media and other online platforms. Privacy has become a vanishing concern, but the private sector has seen this cultural change as an astounding business opportunity. It has given rise to the surveillance economy.

Silicon Valley's giant digital platforms, assisted by a flank of data brokers and marketers, have responded by gathering and analyzing information flowing from our personal computers, mobile phones, credit cards, anything through which data moves. A global industry has arisen that captures, analyzes and makes "actionable" this valuable personal information. The industry buys and sells your data like Wall Street trades stocks, making billions off data dossiers—our profiles. Your profile reveals much about who you are, such as how much you

spend; the products you buy; who you vote for; who is part of your family, including your kids in the home; your health concerns. This ever-growing profile, in turn, is used to generate personalized and micro-targeted advertising messages delivered to any digital device or service you may be using.

This personal information has been a bonanza to the online platforms and their advertisers—both commercial and political. Through connections to friends, services, entertainment and programming carefully designed to go viral, the platforms keep people online by driving content that is intended to engage, provoke and be rapidly shared. This is why another YouTube video starts playing as soon as one ends; why Facebook sends emails letting you know a friend posted something ("View on Facebook"); why Twitter tells you about missed tweets from folks it knows you are following.

Data and Advertising

This content delivery is not random. The user-profiling and recommendation engines are increasingly powered by artificial intelligence software. Super computers help the online advertising system essentially spy on our online lives, assembling profiles and providing those insights to advertisers. Online content is also honed using an array of tools—sometimes called neuromarketing or emotion analytics—to trigger our feelings and psychology. In other words, the backbone of online advertising is a system aiming at our subconscious minds.

Advertising, as a profession, has always been about cultivating illusions to prompt people to buy products— or in politics, ideas and agendas. What is different with the online advertising revolution is that the dominant platforms have given control over an unprecedented range of meticulously detailed user data and content-delivery options to advertisers. This interplay of data and deep personal targeting (online advertising's business model) can blur the distinction between what is fake and what is real. This online system lets advertisers popularize, virally distribute and promote products, trends and political news. But this architecture and its application have also played a role in dividing society and elevating disinformation.

PRIVACY HAS BEEN BREACHED AS NEVER BEFORE. SUPER COMPUTERS PROFILE USERS AND DRIVE CONTENT TO PROVOKE AND BE RAPIDLY SHARED. SOCIETY IS BEEN BROKEN INTO NARROW ECHO CHAMBERS—FILTER BUBBLES.

This result can be seen across society, as people with common interests can find each other online and even withdraw into narrow silos. In the political sphere, this sorting has broken the electorate into narrower and more isolated echo chambers, or filter bubbles. The architecture of online media panders to personal biases, especially partisan vitriol. Its emphasis on more individual tastes

and interests has demoted facts and institutions that rely on accepted gatekeeping and public trust. These trends threaten mental health, journalism, elections and democratic institutions.

This perspective obviously is a dark view of things and not the whole story. But it is essential to be vigilant. This is especially true when you think about the fact that most of us are knee-deep in the same technology systems that are often not playing fair by enabling advertisers and others to bait their users. Many of us have thought of Google, Facebook, Twitter etc. as our friends. They are part of our daily lives. But we probably should reconsider the relationship, if we haven't already. At a minimum we might understand these powerful platforms and social media as our "frenemies."

Admittedly, most of us cannot live without our devices, online tools and digital platforms. This e-book suggests we should question what it means to live with them, be cautious, and question whether sectors of this cyber-system that are antithetical to democratic discourse (such as the ad-based business model) should keep going as they have been going.

At one point there could have been an Internet whose growth and structure was more socially conscious and not exploitive—the utopian, not dystopian, vision. But those who became the major movers of the Internet and built the platforms we all use often came with a libertarian philosophical bent. Their values leaned toward behavior more along the lines of Ayn Rand than Franklin Delano Roosevelt. Their vision was commercial—primarily concerned with generating wealth. They

opposed constraints on data gathering and its use. They eschewed ethical standards. They recited the libertarian ideal of online freedom, rather than shared responsibility and mutual ties.

A Growing Backlash

Why have elections become so fraught? True, in many states, elections have always involved levels of trickery, voter repression, and powerful efforts by those in power to remain in control. But because of the Internet, and the ascendance of social media, something vastly more dangerous is taking place.

There is a growing awareness that the mass-personalized data-gathering advertising business model, and the technology behind the historic growth of Facebook (2 billion users worldwide), Google-owned YouTube (1.5 billion users) and other platforms, has led to unaccountable forces.

Individuals and public institutions have begun to push back. Even if it's simplistic, citizens and bloggers have called for the U.S. government to break up Facebook. In Europe, Google has been fined billions for anti-competitive practices and a sweeping new online privacy law has been passed. Non-governmental organizations (NGOs) in the U.S and Europe keep pushing for more effective measures, including anti-trust action.

Given the concerns, it is fundamental that the public and its elected officials need to better understand the impact of the surveillance economy. When Facebook CEO Mark

Zuckerberg testified to Congress in early 2018, it was apparent most of our representatives did not have a clue about how online media, and specifically social media, worked. They understood there might be a problem, that privacy was threatened, but little else. True, it is complex. But dependable, trusted information can be a counterweight. It helps when we know the problems, and can work together to hold elected officials and companies accountable—or encourage reformers in their midst.

Fortunately, in the U.S., some federal lawmakers are grasping the big picture, the stakes and the scope needed for solutions. Sen. Mark Warner (D-VA), who made a fortune in technology investments, has been studying proposals to promote competition and force the platforms to be more transparent. One would designate key features (such as Google Maps) as critical infrastructure.[45] Such designations could radically restructure some elements of the online economy. But there will be tremendous resistance from industry and its protectors in office. Those industry champions, even in super-majority blue California, have included Democrats—members of Warner's party.[46] Moreover, like all high-stakes political battles, elected officials and their campaigns are in a digital data arms race, where no side wants to be the first to disarm.

The Two Biggest Problems in Elections

There are two overarching developments that have a huge impact on elections, both of which depend on the basic model of the surveillance economy data gathering.

The first problem is that advanced technology makes it possible as never before for campaigns to zoom in on individual voters with distinct messages. New tools have enabled data companies to reach, engage, and micro-target voters with exacting precision. Behind this scrutiny is a powerful corporate sector including data brokers, identity management platforms, marketing clouds, measurement companies, social media and the advertising industry.

The second big problem is the outbreak of junk news and disinformation. Whatever you want to call it, it was rampant on the Internet during the 2016 election. Junk information was widely distributed by campaigns, foreign powers, opportunists, computer robots and others, who sent messages to recipients based on their beliefs, biases and social circles.

THE POWERFUL CORPORATE DATA INDUSTRY INCLUDES DATA BROKERS, DATA MANAGEMENT PLATFORMS, MARKETING CLOUDS, SOCIAL MEDIA, MARKET-MEASUREMENT COMPANIES AND THE ADVERTISING SECTOR.

The mechanics of this micro-targeting and misinformation-distribution can be described. Kathryn Montgomery and Jeff Chester, the *Center for Digital Democracy*'s co-founders, have extensively researched the data industry's techniques. Some are updated versions of long-standing political practices, retooled to be more effective. Others are newer departures, imported directly from the commercial sector and adapted for use in campaigns.

They have identified six major features that the data industry has used in campaigns to influence voters. The best way to understand these features is to look at them as elements in a system that's revolutionized how campaigns and voters interact, which Montgomery and Chester described for the scholarly *Journal Internet Policy Review* in late 2017." A detailed knowledge of these techniques is not necessary for readers of this guide. Here are summaries from their article.

- **Digital dossiers: data mining, profiling and "cloning" the citizenry.** For years, political campaigns have been able to combine public voter files (by state or district) with commercial data from information brokers and platforms like Facebook to develop detailed and comprehensive dossiers on all voters. With recent advances in advertising technology and the data sector, political campaigns have unprecedented tools for data-mining and voter targeting.

- **Geotargeting and geofencing through mobile.** Mobile devices are spies in our pockets. They breach the barrier between one's physical location and online snoops. The phones continually send signals that enable advertisers (and others) to ascertain one's

location. Through a host of location technologies, consumers can be identified, followed and targeted wherever they go: driving a car, pulling into a mall, or shopping in a store. The timing for targeted messages can be fine-tuned for maximum impact.

· **Tracking individuals across devices through the "identity graph."** Digital platforms, data brokers, and advertising technology companies have also developed a number of ways to determine and confirm who a person is. Creating a so-called "identity-graph" has become a key strategy for finding and reaching consumers across all their devices—which helped the private sector to take advantage of the growing dominance of mobile as the primary device.

· **Using automated advertising to identify and micro-target individual voters.** This is automated ad-buying and placement on digital media. The massive growth of programmatic advertising was one of the major changes in online campaigning between 2012 and 2016—"the first time in American history," one leading ad company said, "that such precise targeting has ever been made available at such great scale."

· **Personalizing TV ads.** Television is becoming more like online media for advertisers. New technologies and "addressable" set-top boxes have transformed cable and broadcast TV into micro-targeting tools, capable of delivering the same kinds of granular, personalized advertising to voters. Campaigns use "second-to-second viewing," combined with other data, to fine-tune ads.

The Outbreak of False News

There was an outbreak of deliberately misleading information and political propaganda on online platforms in 2016, often issued with a conspiratorial bent. As noted above, some experts don't want to use the term "fake news" to describe this trend, because Donald Trump uses "fake news" as a label to attack anything with which he disagrees, including fact-checked reporting from *The New York Times* and *Washington Post*.

In general, however, "fake news" has become a label describing a range of problematic content from accidental misinformation to purposely deceptive content. It is also used for outrageous headlines, hate speech, arch partisan content, and other political propaganda. At the Computational Propaganda Project, based at the U.K.'s Oxford Internet Institute, they use the term "junk news," since it "more accurately describes the wide range of bad information that spreads on social media through the powerful algorithms of companies such as Google, Facebook and Twitter."[48]

The idea of false news has risen to prominence in what's now being called a "post-truth world." The Oxford English

JUNK NEWS, FALSE NEWS, DISINFORMATION, FAKE NEWS. CALL IT WHAT YOU WANT, BUT IT'S PROPAGANDA AND OFTEN EXTREME, OFTEN MISLEADING AND OFTEN CONSPIRATORIAL.

Dictionary named "post-truth" as its 2016 word of the year, saying it was an adjective "relating to or denoting circumstances in which objective facts are less influential in shaping public opinion than appeals to emotion and personal belief."[49]

Stanford's Persily, a nationally known legal scholar of online media and democracy, has studied the dangers to democracy that have emerged as online media has moved to the center of campaigns. Here are some of his takeaways from an insightful 2017 article in the *Journal of Democracy*:[50]

- False news can originate from official campaigns, anonymous allies, friendly media and their web sites, candidates and even foreigners.

- Aided by online platforms, fake news ricochets among campaign nodes, moving online and offline as campaigns, supporters and media repeat the stories.

- The speed and scale at which content "goes viral" grows exponentially, regardless of whether or not the information it contains is true.

- The complexity of the network that produces and retransmits fake news makes it hard to pinpoint the source of a false claim.

- The pace with which lies can travel in the online world versus offline is much greater as technologies such as automated social media bots and other delivery systems are developed and deployed.

- Social-media bots can spread lies to people who will believe them.

- The power of fake news is often determined by the viral spread of the lie that's propagated, the speed with which it is disseminated without timely contradiction, and how many people receive and believe the falsehood.

- Academic evidence suggests that viewers have considerable difficulty distinguishing between real and fake news, and trust in traditional media outlets is at an all-time low.

- Fake news cannot only change voter attitudes toward issues and candidates, but it can demobilize voters by fanning cynicism. False stories create a blanket of fog that obscures the real news and information put out by campaigns.

- The premium placed on virality, the threat to accountability posed by unrestrained anonymity, and the undercutting of sovereignty presented by an open Internet pose novel challenges for democracy in the United States.

"The politics of never-ending spectacles cannot be healthy for a democracy," Persily wrote. "Nor can a porousness to outside influences that undercuts the sovereignty of a nation's elections. Democracy depends on both the ability and the will of voters to base their political judgments on facts, or at least on strong intermediary institutions that can act as guardrails to channel decision making within the broad range of democratic alternatives."[51]

What Can We Do to Protect Ourselves?

Introduction

T There are things we can do to protect ourselves from being targets for online political advertising, false news and disinformation. There are practical steps individuals can take. Social media corporations and regulatory bodies must also step up to confront their effect on political culture and public life, including their impacts on many aspects of economic and private life.

As individuals, we will need to be more aware of what information is being spread, developing a higher level of what many call media literacy. We need to find better ways to spot and resist false information. We can also be in a stronger position to push public officials and private corporations to rein in the surveillance economy's excesses that are invading our privacy and harming our politics.

The good news is there is a growing recognition in serious circles about the dangers and their wider impacts—including economic stakes. As Sinan Aral noted in Harvard Business Review in August 2018, "False news affects our economy, our investments, and the value of individual businesses. In 2014 a false tweet claiming that Barack Obama had been injured in an explosion wiped out $130 billion of equity value in a single day."[52]

"THE IMPORTANCE OF UNDERSTANDING THIS PHENOMENON IS DIFFICULT TO OVERSTATE. AND, IN ALL LIKELIHOOD, THE PROBLEM WILL GET WORSE BEFORE IT GETS BETTER."

"The importance of understanding this phenomenon is difficult to overstate," Aral and co-authors wrote for Science magazine. "In all likelihood, the problem will get worse before it gets better, because the technology for manipulating video and audio is improving, making distortions of reality more convincing and more difficult to detect." [53]

Advertisers and media outlets have to be challenged about the consequences of spreading falsities. They have to force producers of fake news off their platforms and step up to slow or halt its spread. It is remarkable that it was not until August 2018 that Facebook, YouTube and Apple Podcasts took down right-wing provocateur and conspiracy fabricator Alex Jones' InfoWars program —which claimed the mass shooting at Sandy Hook Elementary School was staged by the government, among other lies. After much hand-wringing,[54] Twitter banned Jones for a week in mid-August.

Part of the challenge for the online media corporations will be to develop effective algorithms to help identify false news and understand better how it spreads. To its credit, Facebook has instituted transparency rules for 2018's political advertisers[55] and some privacy protections[56] for its users. Its steps include creating a searchable archive of political ads posted since May.[57]

Ongoing congressional hearings into Russian meddling in 2016 have also prompted some lawmakers to study solutions that could be far reaching, including Sen. Warner's above-mentioned proposal to designate key online media components, such as Google Maps, as "essential facilities" and require their owners to provide

third-party access to their data.[58] Congressional staffs have also discussed electioneering disclosure requirements and penalties for publishing false news.[59] Online advertising transparency legislation has also been introduced.[60]

None of this will be easy to achieve in America, however, as there is a constant debate about what is truth and even a growing disagreement about "facts" The First Amendment's political speech protections are frequently cited as a reason to do nothing and to criticize anyone who seeks new regulations. As Aral asks, "How can we disincentive the spread of falsity, and incentivize the spread of good-faith communications and truth?"[61]

The steps we can take begin with protecting our privacy and reducing the amount of data being collected about us, our families and friends. But it is important to be aware of how hard it will be to avoid online propaganda and protect our privacy if we continue to use the Internet— from search engines to social media.

There is a radical solution to false news and the surveillance economy proposed by tech visionary Jaron Lanier in his recent book, *Ten Arguments for Deleting Your Social Media Accounts Right Now*.[62] Lanier urges people to quit social media and avoid the surveillance mechanism that the Internet has become. Lanier's underlying argument is stark: What has suddenly become normal in the past five-to-10 years is "persuasive surveillance and constant, subtle manipulation — and it is unethical, cruel, dangerous and inhumane." He asks: Is this truly dangerous? And answers: "Oh yes, because who knows who's going to use that power and for what."

Some will be tempted by Lanier's arguments. His book is entertaining and sobering. It provides a dark view of technology's impact on societies around the globe. However, most of us can't drop out of the digital-media world because of work, family, or our dependence on the many ways this technology makes our lives easier. It can give us the entertainment we want. In some cases, technology doesn't frighten us enough to do something about it.

Media Literacy's Big Caveat

There is a big caveat for those who take steps to protect their privacy from intrusive corporations and governments, unwelcome political ads, annoying fund-raising appeals, and false or intentionally provocative content. Even if you shut down your personal online exposure to political opportunists, you likely will still see inflammatory messages sent by your social media peers, friends, relatives, work colleagues or news sources.

The technology sector has gathered so much information about everyone that it's almost impossible to escape being a known quantity. In August 2018, Simon Balfe, a manager at Google Marketing Solutions, told a trade journal, "what Google's machine learning can do is, look at 17m [million] signals every time somebody [an advertiser] types in a search query and … use all that detail to see how likely somebody is to take that action." The predictive data variables included time of day, the device the targeted recipient was using, and their "previous behavior."[63]

GOOGLE LOOKS AT 17 MILLION DATA POINTS EVERY TIME AN ADVERTISER TYPES IN A QUERY TO SEE HOW A TARGETED PERSON IS LIKELY TO REACT.

The first line of digital defense is a healthy skepticism about anything that comes through the digital door. "A lot of that targeting doesn't necessarily come from data collected from you," explained Danny O'Brien, international director of the Electronic Freedom Foundation (EFF). "It just comes from people having a fairly accurate view of what people like you might be interested in or might get them upset."[64]

"In that situation, the strategy is really a certain degree of media literacy, writ large, about what's going on. It's sort of a matter of understanding that Facebook is picking these things out for you, and Twitter is optimizing for the amount of engagement that you have with it. The solution isn't very technical. The solution to that is diminishing your involvement with social media platforms that have that attitude toward you."

O'Brien also suggests using tools to block the spying of the surveillance economy (discussed under Privacy below). His advice doesn't deal with the fundamentals of online advertising's business model, but that larger task is coming before governments—particularly in the European Union. The E.U. is now implementing the strongest online privacy law on the planet—one unambiguously returning control over users' data to users—not platforms.

That law, called the General Data Protection Regulation, took effect on May 25, 2018.[65] It directly challenges social media platforms' abilities to micro-target voters in political campaigns. Because Silicon Valley giants are global businesses, the biggest online media platforms cannot ignore the GDPR.

Meanwhile, in mid-July, the California Legislature passed the strongest state digital privacy law[66] in the country—prompting other states to launch hearings on the issue. However, California's law—opposed by every major industry in the state, from tech to banking to movies—won't take affect until 2020. It imposes rules on an online business world that ignored privacy issues and the ethical implications.

UPDATED PRIVACY SETTINGS WILL CUT DOWN ON YOUR BEING TARGETED BY PARTISAN CAMPAIGNS.

People need to look at what governments are doing. What is required is that states and the federal government enact privacy laws that stop political campaigns and commercial marketers from so easily taking advantage of all our information. Significant controls must be enacted.

But we also need to control our own data—to the greatest extent possible. That starts with using the privacy settings on the major online platforms to blur what is traced, profiled and ultimately sold to any political campaign or business.

Privacy

O rganizations like the Electronic Frontier Foundation[67], *TechSolidarity.org*[68] and *AccessNow.org*[69] have created resources and tools for people who need or want to protect themselves from government surveillance—which is not the same as private corporate data mining. Their checklists are revealing, informative and begin to show the difficulty of this challenge. Their advice also holds for anyone working on campaigns, because they need to protect themselves from meddling from opponents or trolls.

Tech Solidarity's basic advice starts with not sending anything sensitive by email. Don't store sensitive information in the cloud. Don't use fingerprints to unlock devices. Don't use a phone number to recover passwords, nor take digital devices you work on across international borders. Do not use an Android phone. That's not all. They say don't plug into an unknown data port, such as an airport charging station, without further security precautions. The additional precautions are long passwords, security keys, two-factor authentication, and avoiding laptops in favor of iPhones and iPads, or Chromebooks for Windows. And there are more steps: EFF suggests one should use encryption at home and at work, virtual private networks if possible, and secure browsers like Tor.[70]

But large numbers of American journalists don't follow these suggestions, to say nothing of the general public. It's virtually impossible for anyone whose business depends on the information ecosystem to avoid search engines, or

to track advise that analysts, public officials and activists are posting on Twitter, which is like a 21st century press release service.

For example, at the bottom of the Twitter settings menu is a button labeled Your Twitter Data. If you click it, you will see how many advertisers have your data—for one inquisitive *New York Times* business reporter it was 600.[71] That settings menu is where you can begin opting out of, or turning off, this so-called interest-based advertising tool.

There's a similar option for Facebook. First you find the Settings menu and look for a tab labeled Ads, which, in turn, reveals the advertisers that have targeted you and, via a drop-down menu, allows you to opt out of being shown ads based on your personal profile.

There are other steps that technical experts suggest you try to stop advertisers from stalking you online.[72] First, the experts suggest periodically clearing the cache of cookies in your browser, as that is a repository of tools for advertisers. In a similar vein, both Android and Apple phones allow users to reset their advertising IDs. On Android phones, this is found inside the Google Settings app. On iPhones, it is inside the Settings app in the privacy menu. Google also has a "My Activity" tool (myactivity.google.com) where you can look at what the company has collected about you, and delete elements.

There are also software apps and other browsers that screen and block ads that follow you around. These include Firefox Focus, DuckDuckGo and Ghostery Privacy Browser. But if you install some of these apps, you might have to temporarily turn them off to be able to use some

websites—such as the email systems communicating with your health-care providers.

These steps will not make all ads on these social media platforms disappear. But the overall mix may become more generalized, as opposed to targeting political beliefs and biases. That's due to several reasons. The platforms themselves have not altered their ad-based revenue model or micro-targeting abilities. Nonetheless, if you turn off these data-revealing and sharing options, you will see fewer political ads. When you turn those options back on, the political ads will reappear.

Facebook also developed new policies to demote political content that independent fact-checkers have found to be distorted or false,[73] remove pages based on fabricated content,[74] and ban repeat offenders.[75] Facebook also imposed disclosure requirements on whoever is buying political or issue ads,[76] and created an online archive of political ads posted since spring 2018.[77] These steps are designed to limit how propagandists and provocateurs can use the world's largest social media platform.

These responses are controversial, because some go further than what Congress has previously done. But a big schism remains in the U.S. when it comes to government involvement. Both political parties have appropriated millions to secure voting systems from Russian hacking in 2018, but neither will do much of anything to address the outbreak of false news or content that tries to push political activism into inciting conflict.

Where We Are

With the 2018 midterms quickly approaching, followed by the presidential campaign season, voters will have to be vigilant to see through the partisan and media fogs. This is true, even as Facebook and Twitter have responded to Russia-centric criticism with tools and policies[78] to block fake accounts, censor false news and blunt bot-led attacks—steps that are still evaded by many determined bad actors. But these steps are progress compared to the online media landscape of 2016.

This guide's purpose is to expose online media manipulation, help people understand the reasons it came about, understand what it means to be citizens in a surveillance-driven online ecosystem, and prepare readers for the near future. There have been, for example, some astute warnings about which slices of society are likely to be targeted for misinformation campaigns during 2018's midterm elections.

In August, Philip Howard, director of the Oxford Internet Institute, testified before the Senate Intelligence Committee and said that much of the racist, misogynist, bullying that marked 2016 will likely continue.

"Within the United States, we can expect the same kinds of [swing district] voters to continue to be targets for misinformation," Howard said. "Given the disinformation campaigns which have been—and are currently—running, I would guess that foreign actors will continue to aim future disinformation campaigns at African American voters, Muslim American voters, white

supremacist voters, and voters in Texas and the Southern States. I expect the strategy will remain the same: Push disinformation about public issues; discredit politicians and experts; and prevent particular types of voters from participating on Election Day."[79]

2018'S PROPAGANDISTS "WILL CONTINUE TO AIM FUTURE DISINFORMATION CAMPAIGNS AT AFRICAN-AMERICAN VOTERS, MUSLIM-AMERICAN VOTERS, WHITE SUPREMACIST VOTERS, AND VOTERS IN TEXAS AND THE SOUTHERN STATES."

This is a sobering forecast. But voters, government and Silicon Valley can make conscious choices if we are not going to normalize extremism. The challenge is not just about the next election, but fortifying democracy against sophisticated and powerful forces that are fanning extremism and conflict. Greater media literacy is one step. Protecting online privacy and regulating the online giants are two more. So too is challenging the online platforms to be better—as their technology can advance our democracy or help pull it apart.

This complex landscape is what voters face in 2018's midterm election and the 2020 presidential season that will begin soon after. It presents unique challenges for voters, for governments concerned about representative democracy, and for Silicon Valley's giants—since civil society starts in the public square that they have colonized and, in many respects, control.

Glossary

CLICKBAIT

Virtually everyone has succumbed to clickbait and often many times over. These are the are headlines, texts or links that can be tantalizing or sexy, that can invoke fantasies, make you curious or angry, spark a range of emotions—whatever grabs your attention. Click on the link and it is likely to lead to an advertisement, or to a site where you will be viewing advertisements where your eyeballs produce income for the website, or even trap you in malware territory.

The clickbait headline has become a symbol of what some fear is the deterioration of journalism. Publishers needing traffic for income or to get important information to large audiences have resorted to clickbait. There is massive competition for attention on the Internet, (with, of course, cat videos at the top of the attraction food chain). This means journalism has had to shift to compete—with some good results and arguably plenty of bad consequences.

COOKIES AND ADVERTISING IDS

Cookies are snippets of computer code that track personal information when one visits a website to enable the site to identify and track the visitor. Often cookies are essential for web sites to keep track of you when making purchases, or to identify you when you come to the site for quick access. But cookies also enable recommendations from visited web sites based on previous behavior or visits to other sites. Other so-called "persistent identifiers" that can help track you on mobile phones, such as advertising IDs, are also used. Increasingly all the trackers are "merged" to help marketers, including political campaigns, target you by using a combined single ID.

Glossary

ALGORITHMS

Algorithms can determine what news, information and online ads you will receive by sorting and filtering the vast amount of content aimed at you. The filtering maximizes engagement, your time spent on the platform, and response to ads. These algorithms' goal is to personalize the delivery of information based on tracking and analyzing your habits and interests, and the habits of people that the algorithms have deemed are similar to you. Reformers want social media algorithms to be more transparent, but that is a difficult struggle because they are proprietary—trade secrets. Many experts criticize the structure of the algorithms because they can end up producing what are called filter bubbles, or echo chambers that can reinforce prejudice and bias.

FILTER BUBBLES

A filter bubble is an odd name for what some social media algorithms tend to do, which is to segregate like-minded people by filtering information served up by their friends, networks, and websites they like to visit. The criticism, in part, is that this practice makes it harder to find diverse opinions because it will not offer you information that you may disagree with. In the political sphere, this can be very troubling because one might get decidedly one-sided perspectives when information is not distributed evenly.

The bubble may seem harmless at first, but the result tends to polarize the public, stifling debate and perhaps exacerbating prejudices by creating a psychological issue called "confirmation bias," which can affect people of all ideological stripes. Partisan bubbles have many destructive political effects. When voters do not get representative, balanced or accurate news, the basis for governing, legislative compromise and solving problems is undermined.

Glossary

BOTS

One way junk news stories spread across social media was through the use of "bots," which is slang for automated computer robots. These are algorithms, or coded instructions, that operate over social media and seek to mimic the reposting or sharing of content from real people. They have been employed to manipulate public opinion across a range of social media and devices. This is a key way junk news is spread online. Bots are particularly active on Twitter and Facebook. They are often designed to boost the number of followers or retweets of hashtags (user-generated search terms). Research suggests that bots played a disruptive role in the 2016 election, with some claiming that bots accounted for 20 percent of all the tweets during this period.

CONFIRMATION BIAS

Confirmation bias happens when a person looks for, notices and prefers information that confirms his or her beliefs. In contrast, a person may ignore, or undervalue the importance or relevance of what contradicts his or her beliefs and worldview. Confirmation bias is especially prevalent during elections because confirming messages can give one confidence in decisions, reducing reasons to consider other candidates, points of view or complexities.

Confirmation bias also allows us to avoid cognitive dissonance, i.e., the discomfort or stress that can accompany trying to hold contradictory ideas, beliefs or values. Confirmation bias can be part of common psychological concepts such as denial, cherry-picking facts, or selective thinking, which are all mental shortcuts that help enable cognitive biases. One cognitive bias prevalent in elections is called the Dunning-Kruger effect, in which people with poor information or cognitive skills have the illusion that their skills and information are better than they are.

Glossary

DARK POSTS

Dark posts are online feeds, messages or ads that can be seen by no one but the person being targeted. Increasingly, dark posts are being used in political campaigns as thousands of ads are tested and tweaked to increase individual responses. It is now possible to send targeted television ads to individual voters based on their preferences and beliefs contained in their online advertising profiles.

POST-TRUTH SOCIETY

Representative democracy, at least in theory, depends on the consent of the governed. But when voters with opposing beliefs and interpretations cannot agree to the basic facts surrounding any real-life event, what can emerge are political gridlock, greater partisan polarization and the potential for conflict.

The Oxford English Dictionary named "post-truth" as the 2016 word of the year, saying it was surfacing mostly in political contexts. They defined this adjective as "relating to or denoting circumstances in which objective facts are less influential in shaping public opinion than appeals to emotion and personal belief."[80] They cited 2016's Brexit vote in the U.K. and the American presidential election, saying "the new implication [was] that truth itself has become irrelevant."

About the Authors

CENTER FOR DIGITAL DEMOCRACY

The Center for Digital Democracy reviews and addresses the activities of the commercial digital media industry, including the leading platforms as well as data, advertising and marketing companies that shape our online experiences. The Center investigates practices that undermine the democratic potential of the digital media as well as threaten the interests of consumers. CDD has played a leadership role for nearly three decades promoting the need to protect privacy and ensure consumer protection on the Internet.

JEFF CHESTER

Jeff Chester is Executive Director of the Center for Digital Democracy. A former investigative reporter and independent producer, Chester has been at the forefront of campaigns to hold the digital media accountable to policymakers and the public. He is the author of Digital Destiny: New Media and the Future of Democracy (The New Press, 2007) and other publications.

STEVEN ROSENFELD

Steven Rosenfeld is a senior writing fellow of the Independent Media Institute, where he covers democracy issues and edits **Voting Booth**, examining the electoral process and political culture. He is the author of several books on elections, most recently Democracy Betrayed: How Superdelegates, Redistricting, Party Insiders, and the Electoral College Rigged the 2016 Election (March 2018, Hot Books).

Endnotes

1 Bloomberg

2 Washington Post

3 Bloomberg

4 The Guardian

5 Politico

6 Taylor & Francis Online

7 Epolitics

8 Statista

9 Bloomberg

10 Buzzfeed News

11 Epolitics

12 Journal of Democracy

13 Twitter and Tear Gas

14 Journal of Democracy

15 New York Times

16 Alternet

17 Politifact

18 Bloomberg

19 Bloomberg

20 Fortune

21 Pew Research Center

22 Journal of Democracy

23 New York Times

24 Buzzfeed News

25 Justice.gov

26 Wired

27 Medium

28 Medium

29. Journal of Democracy

30 New York Times

31 New York Times

32 Oxford Internet Institute

33 New York Times

34 Axios

35 U.K. Parliament

36 New York Times

37 New York Times

38 New York Times

39 Oxford Internet Institute

40 New York Times

41 Bloomberg

42 New York Times

43 The Guardian

44 Center for Digital Democracy

45 Axios

46 New York Times

47 Internet Policy Review

48 Oxford Internet Institute

49 Oxford English Dictionary

50 Journal of Democracy

51 Journal of Democracy

52 Harvard Business Review

53 Science Magazine

54 New York Times

55 Facebook Business

56 Facebook Newsroom

57 Facebook Business

58 Axios

59 Axios

60 Sunlight Foundation

61 Harvard Business Review

62 Jaron Lanier

63 Silicon Republic

64 Electronic Frontier Foundation

65 Wired

66 New York Times

67 Electronic Frontier Foundation

68 Tech Solidarity

69 Access Now

70 Tor Project

71 New York Times

72 New York Times

73 Facebook Newsroom

74 Facebook Newsroom

75 Facebook Newsroom

76 Facebook Newsroom

77 Facebook Business

78 Recode

79 U.S. Senate

80 Oxford English Dictionary

LEARN MORE. TAKE ACTION.

DEMOCRATICMEDIA.ORG